ABSTRACT

A method of digital media copy protection is disclosed. The method of the present invention is applicable to any type of digital media data and makes no assumptions on any specific media properties. The method includes a process of protecting digital media data with a public key using a hybrid cryptographic technique, a process of watermarking the media data, and an output device compliance testing process through an authenticated handshake protocol. Because of the media data protection with the hybrid cryptographic technique, a non-compliant playing device is not able to play or read a protected media data set. The output device compliance testing protocol is used to prevent the media signal from being copied to any non-compliant device. These features of the present invention are used to reduce the possibility of making any illegal copies on any nonstandard equipment. In addition, the data watermarking is used to modify the played and recorded media signals, to keep track of the identification information of the related devices for detecting any illegal copy maker, and to separate legal media data sets from the illegal data sets.